

**BOX ISSUE FEE**

**PATENT**

Agent's Docket No. 94680-US

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of	)	ALLOWED: 06/20/00
	)	
John BURNS et al	)	BATCH NO. 034
	)	
Serial No: 09/013,021	)	Art Unit: 2738
	)	
Filed: 26-January-1998	)	Ex: QURESHI, A.
	)	

For: **SWITCHED CONNECTIONS DIAGNOSTICS IN A SIGNALLING NETWORK**

September 14, 2000

Commissioner of Patent and Trademarks  
Washington, D.C. 20231


**OK to Enter**

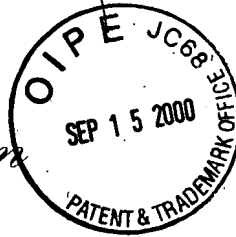
**SUBMISSION OF CERTIFIED COPIES OF PRIORITY**  
**APPLICATION IN SUPPORT OF CLAIM TO PRIORITY UNDER 35**  
**USC 119**

Sir:

We are submitting herewith the priority document in respect of the above-referenced U.S. patent application namely, Canadian Patent Application No. 2,195,893.

Respectfully submitted,

BY:   
Richard J. Mitchell  
Reg. No. 34,519  
Agent of Record



*Bureau canadien  
des brevets*  
Certification

*Canadian Patent  
Office*  
Certification

La présente atteste que les documents  
ci-joints, dont la liste figure ci-dessous,  
sont des copies authentiques des docu-  
ments déposés au Bureau des brevets.

This is to certify that the documents  
attached hereto and identified below are  
true copies of the documents on file in  
the Patent Office.

Specification and Drawings, as originally filed, with Application for Patent Serial No:  
**2,195,893**, on January 24, 1997, by **NEWBRIDGE NETWORKS CORPORATION**,  
assignee of John C. Burns, Stephen C. Bews, Jonathan L. Bosloy and David Watkinson, for  
"Switched Connections Diagnostics in a Signalling Network"

*S. D. Lagore*  
Agent certificateur/Certifying Officer

May 14, 1998

Date





Ottawa Hull K1A 0C9

(21)	(A1)	2,195,893
(22)		1997/01/24
(43)		1998/07/24

(51) Int.Cl. <sup>6</sup> H04L 12/26; H04L 12/56

(19) (CA) **APPLICATION FOR CANADIAN PATENT** (12)

(54) Switched Connections Diagnostics in a Signalling Network

(72) Burns, John C. - Canada ;  
Bews, Stephen C. - Canada ;  
Bosloy, Jonathan L. - Canada ;  
Watkinson, David - Canada ;

(71) Newbridge Networks Corporation - Canada ;

(57) 6 Claims

Notice: This application is as filed and may therefore contain an incomplete specification.



2195893

ABSTRACT OF THE DISCLOSURE

A method is disclosed for diagnosing faults in a network. The network has a plurality of nodes through which switched virtual connections can be established. First, all attempts at establishing routes through the network are recorded. Then, the location of a failure is determined by analyzing the attempted routes.

## SWITCHED CONNECTIONS DIAGNOSTICS IN A SIGNALLING NETWORK

This invention relates to the field of digital networks, for example, asynchronous transfer mode networks, and more particularly to a method and apparatus for diagnosing switched connections in a signaling network.

Network switches controlled by signaling software dynamically set up end to end connections across the network via SVCs (Switched Virtual connections or SPVCs Switched Permanent Virtual connections). Sometimes these connections fail to route successfully. Today's signaling software provides very simple cause and diagnostics information to aid in trouble shooting failed call attempts. Often, the cause and diagnostics are inadequate to trouble shoot the root cause of the problem as only a single reason is provided as to the failure. Much manual work, often involving more than one operations person, must be done, to actually locate the root cause of the problem. This becomes very costly in terms of network resources and time. More detailed connection diagnostics are required to aid in troubleshooting in these situations.

An object of the present invention is to alleviate this problem.

According to the present invention there is provided a method of diagnosing faults in a network having a plurality of nodes through which switched virtual connections can be established, comprising the steps of recording all attempts at establishing routes through the network; and analyzing the attempted routes to determine where a failure has occurred.

The present invention collects details for each switch and physical trunk visited plus rejection causes for every attempted route during the call setup phase and presents this information to the operator. These details enable network operators to easily isolate and troubleshoot problems.

This invention enables signaling software to gather detailed information for a switched connection for every leg of a call rather than simply providing one reason as to routing failure, thus allowing quick problem resolutions with minimal effort.

The invention will now be described in more detail, by way of example, only with reference to the accompanying drawings, in which:-

Figure 1 is a diagram of a network capable of establishing switched virtual connections; and

Figure 2 shows the Diagnostics Points of Failure;

Figure 3 illustrates the Call Trace Of a Successful Call

Figure 4 illustrates a Call Trace Of a Successful Call With One Node Failure; and

Figure 5 illustrates a Call Trace Of an Unsuccessful Call.

In Figure 1, tgXY represents a trunk group from node X to node Y, A, B, E are network switches and uX represents a user for UNI (user network interface) at node X. The nodes are typically Newbridge Networks Corporation 36170 switches.

A switched connection can be setup from CPE-1 to CPE-2 using Users uA and uD for the calling and called addresses, respectively. Alternatively, an SPVC path can be setup from the port on A where CPE-1 is attached at uA to the port on D where CPE-2 is attached at uD. If a routing problems occurs with the switched connection (SVC or SPVC path), then the following steps should be taken to diagnose the problem depending on the type of connection.

#### SVC Case:

A customer at CPE-1 complains his application is not working. The Service Provider turns on switched connection diagnostics for user uA and instructs the customer to try his application again. When the SVC is retried, switched connection diagnostics are collected. The results are analyzed and routing reject points can then be further investigated to locate the problem. The service provider locates source of problem and fixes it. The Customer retries his application and is once again happy.

#### SPVC Path Case#1: Path is *Waiting For Resources*

The Service Provider configures an SPVC path from uA to uD and connects it. The path goes into the *Waiting For Resources* mode. The Service Provider turns on switched connection diagnostics for the specific problematic SPVC path to initiate a SPVC path diagnostics operation. The SPVC path is retried; switched connection diagnostics are collected. The results are analyzed and routing reject points can then be

further investigated to locate the problem. The service provider locates source of problem and fixes it. The SPVC path is retried and goes *Connected*.

SPVC Path Case#2: Path is *Connected*

The Service Provider configures an SPVC path from uA to uD and connects it. The path goes *Connected*. The Service Provider wants to know why the path took the route that it did.

A Bridge&Roll Optimise operation is performed on the path so that switched connection diagnostics can be gathered for the path. This operation may be affect service. However, if done close to the time the path was first connected, then there is a good chance that there is not a more optimal route. The results are analyzed and routing reject points can then be further investigated to discern why the path routed the way it did.

For a specific example of an application of the signaling diagnostics, assume each switch has static routing tables allowing uA to route an SVC to uD, and assume tgCD has no remaining bandwidth for the SVC. The SVC would start from A, use tgAB (assume primary) to get to B, then proceed to use tgBC to get to C. Once at C, routing determines that tgCD is full and cranks back to B. B then cranks back to A as there are no other routes from B to D. A crankback occurs when a node passes a call back to a previous node because it is unable to establish an onward connection. From A, the alternate, i.e., tgAE is used. From E, tgEC is used, and again at C, routing determines tgCD is full and cranks back to E. E then cranks back to A as there are no other routes from E to D. Now A has exhausted its routes so the SVC is released back to CPE 1.

Switched connection diagnostics record all routes attempted, i.e., A, tgAB, B, tgBC, C, reject reasons (cause + diagnostics), A, tgAE, E, tgEC, C, reject reasons. If this list is followed, it can be determined that all roads lead to C, but there is NO usable route from C to D. The next step in the procedure is to focus diagnostics efforts at C to determine why tgCD is not usable.

For SVC Switched Connection Diagnostics, SVCs are setup from user terminal to user terminal across the network. The point of attachment into the network from the user terminal defines the entry and exit points for the SVC. The point of attachment is defined

by a Call Processing User and its physical access i.e., its Trunk Group and the controlling signalling link. The switch routes a SVC from the User at the entry point to the User at the exit point. Routing tables, either static or dynamic, present in each node steer SVC setup messages from the source User to the destination User. When routing chooses a route, i.e., a trunk group, the signalling message is sent out the signalling link controlling the trunk group.

Switched connection diagnostics are provided on a per User basis.

Valid Values: Switched connection diagnostics ON/OFF

Default Value: OFF

Conditions: Every calling User that originates a SVC when switched connection diagnostics is turned ON will gather diagnostics information during call setup. This enables an end-user application to startup, allowing it to signal potentially more than one SVC, and diagnostics will gather information on all SVCs originated from the application.

If diagnostics is not turned OFF for a User after a SVC routing problem has been diagnosed, then call setup performance for the User will be degraded as unwanted diagnostic information is collected for every call on the User. To guard against inadvertently leaving switched connection diagnostics ON, diagnostics are gathered for the first 10 SVCs/SPVC paths setup for the User. After 10 calls for the User, the switched connection diagnostics turns itself OFF.

If Switched connection diagnostics is ON for a User, and that User is the destination of a call, there is no effect. Switched connection diagnostics applies only to calls originated by a User.

In the case of SPVC Path Switched Connection Diagnostics, an SPVC path definition contains the source, destination and administrative information for path setup. The SPVC path setup procedure initiates an SVC from the source endpoint towards the destination endpoint and therefore uses the same routing procedures as SVCs. In one.



reference model, the SPVC path endpoints are the ports on the switch where the CPEs (Customer Premise Equipments) are attached. The Users i.e., uA and uD plus port and endpoint information define the endpoints for the SPVC path. Again, routing uses routing tables, either static or dynamic, present in each node steer SPVC setup messages from the source User to the destination User.

Switched connection diagnostics are provided on a per SPVC path basis.

Valid Values: Switched connection diagnostics ON/OFF for the next SPVC path setup attempt..

Default Value: OFF

Conditions: Once switched connection diagnostics has been turned ON for the SPVC path, the next time the SPVC path is setup, diagnostics information is collected for the SPVC path.

When an SVC or SPVC path is setup, routing attempts to route the call from source to destination. It uses loop detection and crankback optimizations to route the call. In this process, many different routes may be attempted. For every route tried, each switch and trunk group traversed is recorded. When a route is rejected, the reason is also recorded. NMTI (Node Management Terminal Interface) or network management can interpret this information to illustrate the routing points of failure.

Routing tables are regenerated and distributed to all nodes running PNNI (Private Network-Network Interface). If a node becomes isolated because the physical access to it fails, then all routes to the isolated node are removed from all routing tables. If node D goes off-line, then the routing table will not have an entry for the Users on node D. Therefore, the routing of an SVC or SPVC path from uA to uD will fail at A and never leave the node. The switched connection diagnostics information will contain node A, and a cause indicating that the destination is unreachable.

If the routing tables are static, much more diagnostic information is gathered as routing attempts to use all configured routes that lead to D. All cause codes recorded at C will indicate that resources are unavailable.

When routing chooses a trunk group, an SVC/SPVC setup request is forwarded out the signalling link that controls the trunk group. Figure 2 depicts the scenarios that can result between two Newbridge 36170 switches:

- 1 Call control forwards the setup message to the local signalling stack.
- 2 The local signalling stack rejects the message and returns failure to local call control.
- 3 The local signalling stack forwards the setup message to the remote signalling stack. The remote signalling rejects the setup message and informs the local signalling stack of the rejection. The remote Call Control engine is not informed whatsoever.
- 4 Remote call control software in the switch on the remote side of the signalling link receives the SVC/SPVC setup message and processes it.

The first and forth points are processed by call control. It logs diagnostics at this level. However, if scenarios two or three occur, then the diagnostic information must reflect this. If the local end rejects the call, then perhaps the Service Card servicing the signalling link is overburdened. If the remote end rejects the call, then perhaps the Service card at the remote end is overburdened. This information pin-points perhaps a troubled Service card.

Diagnostics is collected on a per Service card basis. The Service card, that manages the SVC User and SPVC path, collects switched connection diagnostics information when diagnostics is enabled. The service card can store switched connection diagnostics information for only 50 SVC or SPVC path setup attempts. The 50 most recent setup attempts are stored. This should be sufficient to allow several external network management requests to initiate switched connection diagnostics requests, then subsequently collect the results.

The Enhanced signalling used to carry the diagnostics information will now be described in more detail. Enhanced signalling is achieved by using information elements defined to be in codeset 6, information elements specific to the local network.

ITU-T standardised coding of these information elements is followed. Therefore all information elements contain an information element identifier, a length and an instruction field as shown below .

8	7	6	5	4	3	2	1	Octet
Information Element Identifier								1
1 ext	0	0	1	0	0	0	1	2
Coding Std      Flag      Res      IE action Ind								
Length								3
Length (continued)								4

The contents of the IE instruction field are always coded with a flag of 'follow explicit instructions' and an IE action indicator of 'discard information Element and proceed'.

New information element identifiers are allocated so as to not collide with codeset 0 identifiers.

Codeset 6 information elements are preceded in a message by the broadband locking shift information element. Non locking shift procedures are not supported.

The purpose of the locking shift information element is to indicate the new active codeset of the succeeding information elements. The specified codeset remains active until another locking shift is encountered indicating the new active codeset.

8	7	6	5	4	3	2	1	Octet
0	1	1	0	0	0	0	1	1
Broadband Non Locking Shift Information Element Identifier								
1 ext	0	0	1	0	0	0	1	2
Coding Std      Flag      Res      IE action Ind								
Length of Broadband Non Locking Shift IE								3
Length of Broadband Non Locking Shift IE (continued)								4
1 ext	0	0	0	0	1	1	0	5
spare      codeset identifier								

Coding Standard (octet 2) is coded to indicate ITU-T standardized coding.  
Flag (octet 2) indicates Follow explicit instructions of the action indicator  
IE action indicator (octet 2) indicates discard information element and proceed

codeset Identifier (octet 5) identifies codeset 6

The following Table summarizes the messages used for enhanced signalling procedures.

Message	Reference
Connect	2.1.1
Setup	2.1.2
Release	2.1.3
Release Complete	2.1.4

Coding Rules as specified by the ITU-T and ATM Forum are followed. The following Table specifies information elements used for enhanced signalling. Max length and max number of occurrences are given for each information element.

Bits		Information Element	Max Length	Max no of Occurrences
8 7 6 5	4 3 2 1			
0 0 0 0	0 0 1 1	Call Trace	*	
0 1 1 0	0 0 0 1	Broadband locking shift	5	1

The messages that are affected by the call trace feature will now be described. Message functional definition and information contents are provided. Message content highlights only the information elements required for this feature.

**Connect** This message is used to return call trace information to the originating node on Successful call completion.

Information Element	Reference	Type	Length
Broadband locking shift	2.2	O	7
Call Trace	2.3	O	23 - *

**Release** This message is used to transfer the reason for a routing failure. Information about the routing failure can be carried in either the cause information

2195893

element or optionally the call trace information element. The cause of the routing failure is carried in the cause whereas call trace carries complete information.

Information Element	Reference	Type	Length
Broadband locking shift	2.2	O	7
Call Trace	2.3	O	23 - *

**Release Complete** This message is used to transfer the reason for a routing failure. Information about the routing failure can be carried in either the cause information element or optionally the call trace information element. The cause of the routing failure is carried in the cause whereas call trace carries complete information.

Information Element	Reference	Type	Length
Broadband locking/ shift	2.2	O	7
Call Trace	2.3	O	23 - *

**Setup** This message is used to collect call tracing information inside the call trace IE as the message traverses the network.

Information Element	Reference	Type	Length
Broadband locking shift	2.2	M	7
Call Trace	2.3	M	23 - *

**Call Trace Information Element** The purpose of the Call Trace information element is used to trace progress of a call as it traverses the network. Information relating to the node address, port and rejection causes is collected, as well as extra diagnostic information.

2195893

8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	0	1	1
Call Trace Information Element Identifier								2
1	0	0	1	0	0	0	1	3
ext	Coding Std		Flag	Res	IE action Ind			4
Length of Call Trace IE								5
Length of Call Trace IE (continued)								6
0	0	0	0	0	0	0	1	7* (note 2)
Call Transited Indication								(note 3)
Call Transited Information								7.1* etc
0	0	0	0	0	0	1	0	8* (note 2)
Call Blocked Indication								(note 3)
Call Blocked Information								8.1* etc
0	0	0	0	0	0	1	1	9* (note 2)
Call blocked after Transit Indication								(note 3)
Call blocked after Transit Information								9.1* etc
0	0	0	0	0	1	0	0	10* (note 2)
Call Success Indication								(note 3)
Call Success Information								10.1* etc

Call Trace Information Element contents form an ordered list representing node traversal information in chronological order

The Call Transited Indication (octet group 7) indication notifies the successful traversal of a single node in the network. It includes node and port information, the format of which is shown below.

8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	0	1	
Call Transited Indication								7.1
length								7.2
0	0	0	0	0	0	0	1	7.3
reserved					address identifier			(note 1)
Domain								7.4
Domain (continued)								7.5
Major Node Number								7.6
Major Node Number (continued)								7.7
Slot Number								7.8
Slot Number (continued)								7.9
port number								7.10
Inbound sub-port								7.11
Inbound sub-port (continued)								7.12
0	0	0	0	selection type		0/1 flag		7.13
reserved								
Slot Number								7.14
Slot Number (continued)								7.15
port number								7.16
Outbound sub-port								7.17
Outbound sub-port (continued)								7.18

If the address Identifier indicates a point code follows, then domain and major node number are replaced by a 22 octet binary number to identify the point code.

The Call Transited Indication (octet 7.1) identifies a route success indicator.

The length (octet 7.2) identifies the length of opcode contents excluding length

The reserved (octet 7.3 and 7.13) is coded as zero for inbound and ignored for outbound.

The address Identifier (octet 7.3) identifies the type of node address that follows as specified by the following table.

Bits			Meaning
3	2	1	
0	0	1	CPSS Address
0	1	0	Point code

The Domain (octets 7.4 -7.5) defines the domain part of the CPSS address

The Major Node Number (octets 7.6 - 7.7) define the major node number of the CPSS address.

The first octet pair of the Slot Number (octets 7.8 - 7.9 and 7.14 - 7.15) defines the ingress slot number of the call and the second defines the egress slot number of the call.

The Port number (octets 7.10 and 7.16) identifies the ingress and egress port number of the call.

The Sub-port number (octets 7.11 - 7.12 and 7.17 - 7.18) identifies the inbound and outbound sub-ports. The interpretation of this field is protocol dependent. For cell relay based protocols it defines the Virtual Path Identifier. The first octet pair defines the ingress virtual path of the call and the second octet pair defines the egress virtual path of the call.

The Selection Type (octet 7.13) identifies outbound port/sub-port selection type as specified by the following table.

Bits	Meaning
4 3 2	
0 0 1	preferred
0 1 0	alternate 1

The Flag (octet 7.13) indicates Assigning/Non assigning interface as specified in the following table

Bit	Meaning
1	
1	Assigning
0	Non Assigning

The Call blocked Indication (octet Group 8) notifies a failure of the call to traverse a single node in the network. It includes node and port information. ingress port/sub-port as well as the reason for call blockage.

0	0	0	0	0	0	0	0	0		Octet
Call Blocked Indication									8.1	
length									8.2	
0	0	0	0	0	0	0	0	1	8.3	
reserved					address identifier				(note 1)	
Domain									8.4	
Domain (continued)									8.5	
Major Node Number									8.6	
Major Node Number (continued)									8.7	
Slot Number									8.8	
Slot Number (continued)									8.9	
port number									8.10	
sub-port									8.11	
sub-port (continued)									8.12	
Cause Value									8.13	
diagnostics Newbridge cause value									8.14	
diagnostics Newbridge cause value (continued)									8.15	
length of diagnostics									8.16	
diagnostics									8.17 etc	

Octet  
8.1  
8.2  
8.3  
(note 1)  
8.4  
8.5  
8.6  
8.7  
8.8  
8.9  
8.10  
8.11  
8.12  
8.13  
8.14  
8.15  
8.16  
8.17 etc

If the address Identifier indicates a point code follows then domain and major node number are replaced by a 22 octet binary number to identify the code point.



The Call Blocked Indication (octet 8.1) identifies call blocked opcode

The length (octet 8.2) identifies the length of opcode contents excluding length and identifier

Reserved (octet 8.3) is coded as zero on egress and ignored on ingress.

Address Identifier (octet 8.3) identifies the type of node address that follows as specified in the following table.

Bits			Meaning
3	2	1	
0	0	1	CPSS Address
0	1	0	Point code

The Domain (octets 8.4 - 8.5) Defines the domain part of the CPSS address

The Major Node Number (octets 8.6 - 8.7) defines the major node number of the CPSS address.

The Slot Number (octets 8.8 - 8.9) defines the slot number of the call  
Inbound/outbound identifier refers to this slot. Slot number is defined to be an 11 bit shelf number and a 5 bit slot number.

The Port Number (octet 8.10) identifies the ingress and egress port number of the call.

The Sub-port (octets 8.11 - 8.12) defines the inbound sub-port. The interpretation of this field is protocol dependent. For cell relay based protocols it defines the Virtual Path Identifier.

The Cause Value (octet 8.13) defines the reason for Routing failure. The cause value is associated with the port most recently traversed.

The Diagnostics Newbridge Cause Value (octets 8.14-8.15) defines cause values to aid network diagnostics.

The length of Diagnostics (octet 8.16) defines the length of diagnostics excluding length

The Diagnostics (octets 8.17 etc) defines diagnostic information added to aid the fault finding process.

The Call blocked After Transit Indication (octet Group 9) notifies a failure of the call to traverse a single node in the network. It includes node and port information. Incoming and outgoing port /VPI information may be present. There is always cause information included to indicate what caused the route failure at this point.

8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	1	1	
Call Blocked After Transit Indication								9.1
length								9.2
0	0	0	0	0	0	0	1	9.3
reserved					address identifier			(note 1)
Domain								9.4
Domain (continued)								9.5
Major Node Number								9.6
Major Node Number (continued)								9.7
Slot Number								9.8
Slot Number (continued)								8.9
port number								9.10
sub-port								9.11
sub-port (continued)								9.12
Outbound Slot Number								9.13
Outbound Slot Number (continued)								8.14
Outbound port number								9.15
Outbound sub-port								9.16
Outbound sub-port (continued)								9.17
Cause Value								9.18
diagnostics Newbridge cause value								9.19
diagnostics Newbridge cause value (continued)								9.20
length of diagnostics								9.21
diagnostics								9.22 etc

If the address Identifier indicates a point code follows then domain and major node number are replaced by a 22 octet binary number to identify the point code.

The Call Blocked After Transit Indication (octet 9.1) identifies call blocked after transit opcode.

The length (octet 9.2) identifies the length of opcode contents excluding length and identifier

The reserved (octet 9.3) is coded as zero for egress and ignored for ingress.

The address Identifier (octet 9.3) identifies the type of node address that follows as specified the following table.

Bits			Meaning
3	2	1	
0	0	1	CPSS Address
0	1	0	Point code

The Domain (octets 9.4 - 9.5) defines the domain part of the CPSS address. The Major Node Number (octets 9.6 - 9.7) define the major node number of the CPSS address. Slot Number (octets 9.8 - 9.9 and 9.13 - 9.14) define the slot number of the call (octet 9.10 and 9.15). Port number (octets 9.10 and 9.16) identifies the ingress and egress port number of the call. Sub-port (octets 9.11 - 9.12 and 9.16 - 9.17) defines the inbound sub-port. The interpretation of this field is protocol dependent. For cell relay based protocols it defines the Virtual Path Identifier.

Cause Value (octet 9.18) defines standard cause values as defined in Q2610. Defines the reason for Routing failure. The cause value is associated with the port most recently traversed. The length of Diagnostics (octet 9.11) defines the length of diagnostics excluding length. The Diagnostics (octets 9.22) define information added to aid the fault finding process.

The Call Completed Indication (octet group 7) notifies the successful traversal of a single node in the network. It includes node and port information, the format of which is shown below.

8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	0	1	
Call Completed Indication								10.1
length								10.2
0	0	0	0	0	0	0	1	10.3
reserved					address identifier			(note 1)
Domain								10.4
Domain (continued)								10.5
Major Node Number								10.6
Major Node Number (continued)								10.7
Slot Number								10.8
Slot Number (continued)								10.9
port number								10.10
Inbound sub-port								10.11
Inbound sub-port (continued)								10.12
0	0	0	0	selection			0/1	10.13
reserved				type			flag	
Slot Number								10.14
Slot Number (continued)								10.15
port number								10.16
Outbound sub-port								10.17
Outbound sub-port (continued)								10.18

If the address Identifier indicates a point code follows then domain and major node number are replaced by a 22 octet binary number to identify the point code. The Call Completed Indication (octet 10.1) identifies a call completed opcode. The length (octet 10.2) identifies the length of opcode contents excluding length and identifier. The reserved (octet 10.3 and 10.13) is coded as zero for egress and ignored for ingress. The address Identifier (octet 10.3) identifies the type of node address that follows as specified by the following table.

Bits	Meaning	
3 2 1		
0 0 1	CPSS Address	
0 1 0	Point code	

The Domain (octets 10.4 -10.5) defines the domain part of the CPSS address. The Major Node Number (octets 10.6 - 10.7) defines the major node number of the CPSS address. The Slot Number (octets 10.8 - 10.9 and 10.14 - 10.15). The first octet pair defines the ingress slot number of the call and the second defines the egress slot number of the call. The Port number (octets 10.10 and 10.16) identifies the ingress and egress

port number of the call. The Sub-port number (octets 10.11 - 10.12 and 10.17 - 10.18) identifies the ingress and egress sub-ports. The interpretation of this field is protocol dependent. For cell relay based protocols it defines the Virtual Path Identifier. The first octet pair defines the ingress virtual path of the call and the second octet pair defines the egress virtual path of the call.

The Selection Type (octet 10.13) identifies outbound port/sub-port selection type as specified by the following table.

Bits			Meaning
4	3	2	
0	0	1	preferred
0	1	0	alternate 1

The Flag (octet 10.13) indicates Assigning/Non assigning interface as specified in the following table

Bit	Meaning
1	
1	Assigning
0	Non Assigning

Call tracing will now be described. Call tracing is established at the exchange originating the call to be traced. At this point a call trace IE is inserted into all calls to be traced. It is only explicitly enabled at the point of origin in the network and is implicitly defined to be active by all other nodes in the network if the call trace IE is found to be present.

#### a) Initiating Call Trace

When a new call is initiated, an empty call trace IE is added to the setup message at the originating exchange.

When an outgoing slot/port/sub-port is selected, the call trace IE is modified before the setup message is forwarded. A 'call transited' opcode, containing node address,

ingress slot/port/sub-port and egress slot/port/sub-port is appended to the end of the IE  
Hence the setup message departs the exchange having traced the point of origin.

A copy of the call trace IE with call transited opcode is saved by the originating exchange.

#### b) Successful Call Completion

The originating exchange checks for the presence of the call trace IE in the connect message. If found, the contents of the call trace IE contains a complete trace of the successful call across the network. It can be used by the management layer for diagnostic information at this point. The IE is not forwarded to the originating interface if it does not support enhanced signalling.

#### Actions Required at a Transit Exchange

##### a) Receipt of a Setup Message

Upon successful route selection the setup message is checked for the presence of a call trace IE. If present, a 'call transited' opcode, containing node address, ingress slot/port/sub-port and egress slot/port/sub-port is appended before the message is forwarded to the next exchange, a copy of the call trace IE is saved.

##### b) Receipt of a Connect Message

The connect message is checked for the presence of a call trace IE. If present, the message is forwarded to the preceding exchange without modification to the call trace IE.

If the call trace IE is absent, the exchange checks for a saved copy. If a copy exists it is added, without modification, to the connect message before the connect message is sent to the preceding exchange. In this case we do not have a complete end-to-end call trace.

#### Actions Required at the Destination Exchange

##### a) Receipt of a Setup Message

Upon successful route selection the setup message is checked for the presence of a call trace IE. If present a 'call completed' opcode is appended to the call trace IE. A copy

of the call trace IE is saved. The setup message is then forwarded to the destination. Call trace IE is removed if enhanced signalling is not enabled at the destination interface.

#### b) Receipt of a Connect Message

The connect message is checked for the presence of a call trace IE. If present, the message is forwarded to the preceding exchange without modification to the call trace IE.

If the call trace IE is absent, the exchange checks for a saved copy. If a copy exists it is added to the connect message before the connect message is sent to the preceding exchange.

#### Call Trace For Unsuccessful Call Establishment

Three levels of information can be provided by a node at the point of failure

- A cause value only
- A cause value and Newbridge diagnostics
- A call trace IE

When a failure occurs a release or release complete message is generated by the exchange at the point of failure. The exchange will incorporate one of the three levels of failure information above into the message. It is therefore the preceding node responsibility to process the failure information correctly.

#### Actions Required at the Originating Exchange

##### a) Detection of a call failure at the originating exchange

A call trace IE is inserted into the setup message. When the originating exchange detects that it cannot proceed with the call, a 'call blocked' opcode is appended to the call trace IE. The call trace IE is copied to the call rejection message sent to the originating user when enhanced signalling is enabled to the user.

##### b) Receipt of a Release or Release Complete Message with a call trace IE

The call trace IE is copied, without modification, to the call clearance message to be sent to the originating user. The call trace IE contains a complete trace of the call and can be used by the management layer for diagnostics at this point.

2195893

c) Receipt of a Release or Release Complete message without a call trace IE

The originating exchange checks to see if a call trace IE has been saved for this call. If available, a 'call blocked after transit' is appended. It is then copied to the call clearance message to be sent to the originating user.

d) Call Failure on receipt of Connect

If a call trace IE is present in the connect message, a 'call blocked' opcode is appended. It is then copied to the call trace IE to be sent to the originating user, if enhanced signalling is enabled.

Otherwise the call trace IE that has been saved is copied to the release message. A 'call blocked' opcode is appended to the call trace IE.

If the originating exchange is unable to include a copy of the call trace IE, normal call clearance procedures should be followed.

Actions Required at a Transit Exchange

a) Detection of a call failure at the transit Exchange

When the transit exchange detects that it cannot proceed with the call, then if possible, a copy of the call trace IE included in the setup message should be copied to the call clearance message. A 'call blocked' opcode is then appended to the call trace IE.

If the transit exchange is unable to include a copy of the call trace IE, normal call clearance procedures should be followed.

b) Receipt of a Release or Release Complete Message with a call trace IE

The call trace IE is copied to the call clearance message to be sent to the preceding exchange without modification.

c) Receipt of a Release or Release Complete message without a call trace IE

The transit exchange copies call trace IE that has been saved to the call clearance message to be sent to the preceding exchange. A 'call blocked after transit' is appended to the call trace IE.

d) Call Failure after receipt of Connect



If a call trace IE is present in the connect message, it is copied to the call trace IE to be sent to the preceding exchange. A 'call blocked' opcode is appended.

Otherwise the call trace IE that has been saved is copied to the release message. A 'call blocked' opcode is appended to the call trace IE.

#### **Actions Required at the Destination Exchange**

##### **a) Detection of a call failure at the Destination Exchange**

When the destination exchange detects that it cannot proceed with the call, then if possible, a copy of the call trace IE included in the setup message should be copied to the call clearance message. A 'call blocked' opcode is then appended to the call trace IE.

##### **b) Receipt of a Release or Release Complete Message with a call trace IE**

The call trace IE from the release/release complete is ignored as the call has been successfully completed by the destination exchange. A copy of the saved call trace IE is copied to the call clearance message to be sent to the preceding node.

##### **c) Receipt of a Release or Release Complete message without a call trace IE**

The destination exchange copies call trace IE that has been saved to the call clearance message being sent to the preceding exchange. A 'call blocked after transit' is appended to the call trace IE. This implies that the final call trace IE will contain a call completed opcode followed by a call trace opcode.

##### **d) Call Failure after receipt of Connect**

If a call trace IE is present in the connect message, it is copied to the call clearance message to be sent to the preceding exchange. A 'call blocked' opcode is appended.

Otherwise the call trace IE that has been saved is copied to the release message. A 'call blocked' opcode is appended.

If the destination exchange is unable to include a copy of the call trace IE, normal call clearance procedures should be followed.

#### **Call Trace On Crankback**

#### **Actions Required at the Originating Exchange**

a) Receipt of Release or Release Complete containing crankback and Call Trace IE

If an alternate route is available, the call trace IE is copied to the outgoing setup message and a 'call transited' opcode is appended.

If no alternate route is available, the call trace IE is copied to the release message to be sent to the originating user.

b) Receipt of Release or Release Complete containing crankback only

If an alternate route is available, the call trace IE that was saved is copied to outgoing setup message. A 'call blocked after transit' opcode is appended. When the alternate route is successfully selected, a 'call transited' opcode is then appended.

If no alternate route is available, the call trace IE is copied to the call clearance message to be sent to the originating user and a 'call blocked after transit' opcode is appended.

#### Actions Required at a Transit Exchange

a) Receipt of Release or Release Complete containing crankback and Call Trace IE

If an alternate route is available, the call trace IE is copied to the outgoing setup message and a 'call transited' opcode is appended.

If no alternate route is available, the call trace IE is copied to the call clearance message to be sent to the preceding exchange.

b) Receipt of Release or Release Complete containing crankback only

If an alternate route is available, the call trace IE that was saved, is copied to outgoing setup message. A 'call blocked after transit' opcode is appended. When the alternate route is successfully selected, a 'call transited' opcode is then appended.

If no alternate route is available, the call trace IE is copied to the call clearance message to be sent to the preceding exchange and a 'call blocked after transit' opcode is appended.

The following contains message flow diagrams for various call trace scenarios.

Symbols in the diagram are defined

- User
- Network Node
- ct Call Trace IE
- # Call Transited Indication
- \$ Call Blocked Indication
- @ Call Blocked After Transit Indication
- ! Call Completed Indication
- () 'Contains'

#### Call Trace of a Successful Call

The Figure 4 shows the call trace feature activated for a successful call. Not all signalling messages are shown. Only messages relevant to the call trace feature are shown.

The setup message is originated at user a and progresses through the network along nodes A,B,E before arriving at user b who responds with a connect to indicate successful call completion.

The Figure 4 shows the call trace feature activated for a successful call with one routing failure at a node. Not all signalling messages are shown. Only messages relevant to the call trace feature are shown.

The setup message is originated by user a and traverses a path along nodes A,C,B. At node B a routing failure occurs. The setup message then transverse a path from B through nodes C,D and E till successful call completion is reached to user b. A connect message is then sent back through nodes E,D,C,A to user a.

Figure 5 illustrates a call failure caused by multiple node failures.

2195893

The following scenario assumes for example that route D-E is OOS and cannot be used to route the call.

The call is initiated from user a through node A. It then progresses to node B as the preferred route. Node B rejects due to a resource problem, but does not include a call trace IE. An alternate route of A-D is selected and the call is then progressed to node D, who also rejects the call. The final call trace IE in the release message from node D contains information of the 2 node failures.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of diagnosing faults in a network having a plurality of nodes through which switched virtual connections can be established, comprising the steps of:
  - a) recording all attempts at establishing routes through the network; and
  - b) analyzing the attempted routes to determine where a failure has occurred.
2. A method as claimed in claim 1 wherein diagnostics data are gathered for each attempted route.
3. A method as claimed in claim 2, wherein said data are included in a call set-up message propagated through the network.
4. A method as claimed in claim 2, wherein said data are included in an information element (IE) field forming part of a call set-up message.
5. A method as claimed in any of claims 1 to 4, wherein said network is an ATM network, said nodes comprising ATM switches.
6. A method as claimed in any one of claims 1 to 5, wherein said switched connections are switched permanent virtual connections.

2195893

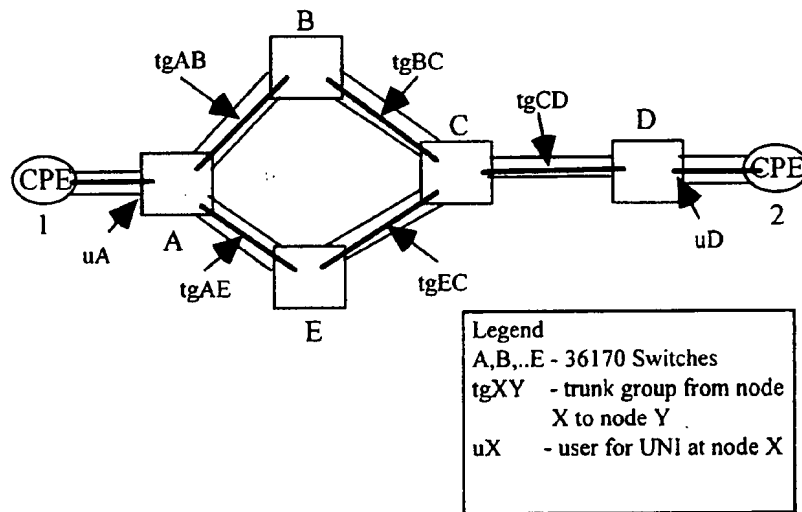


Figure 1

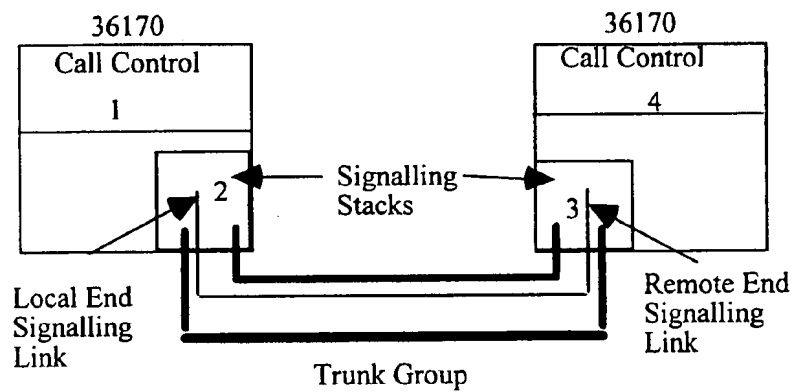


Figure 2

Thanks a Clerk

2195893

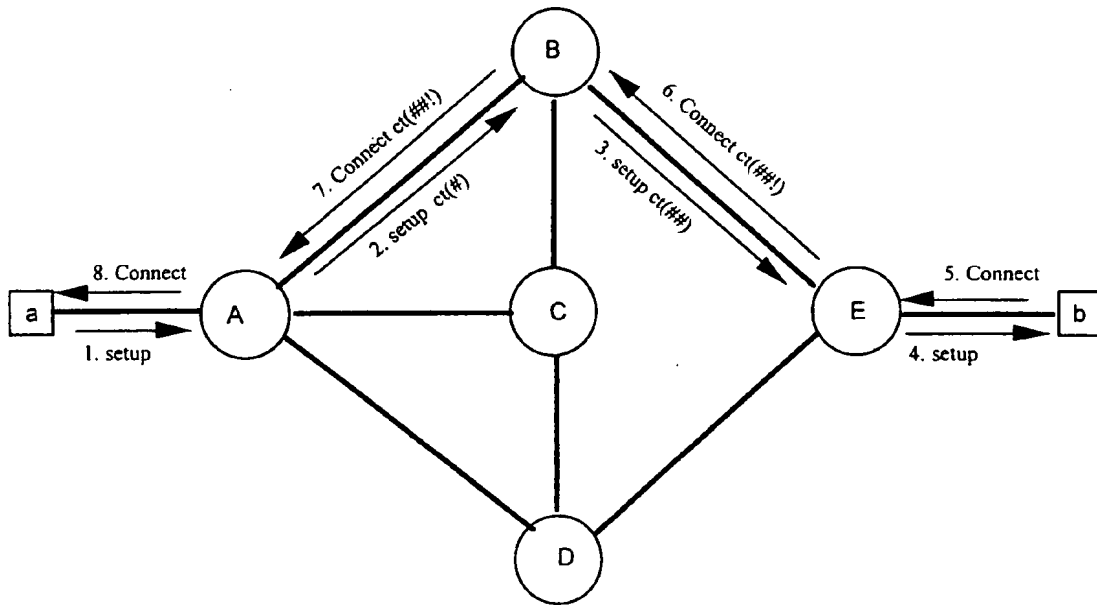


Figure 3

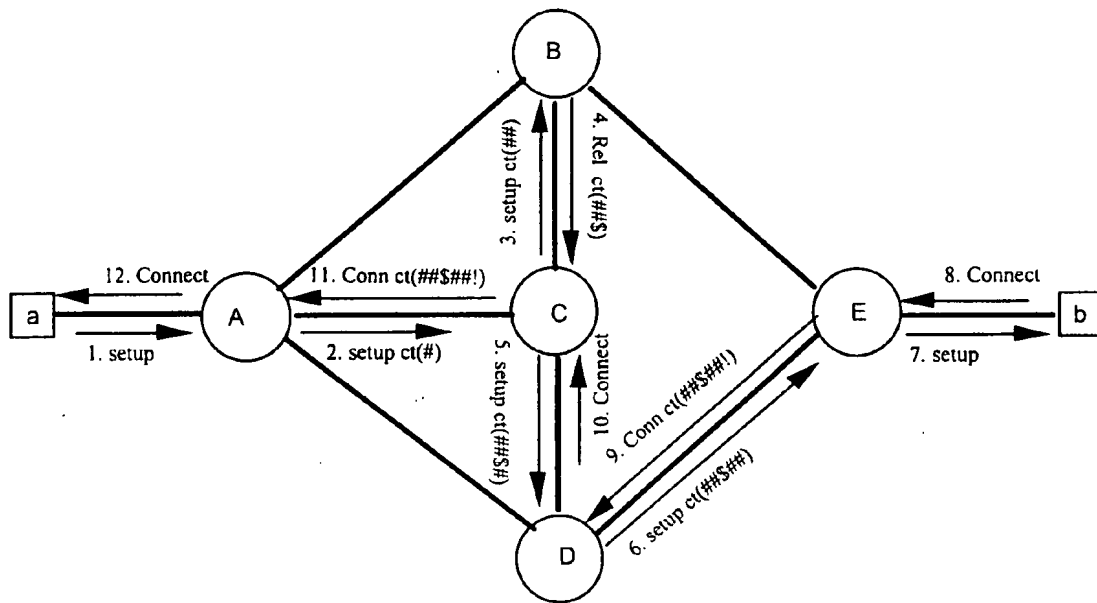


Figure 4

Marko u. Clark

2195893

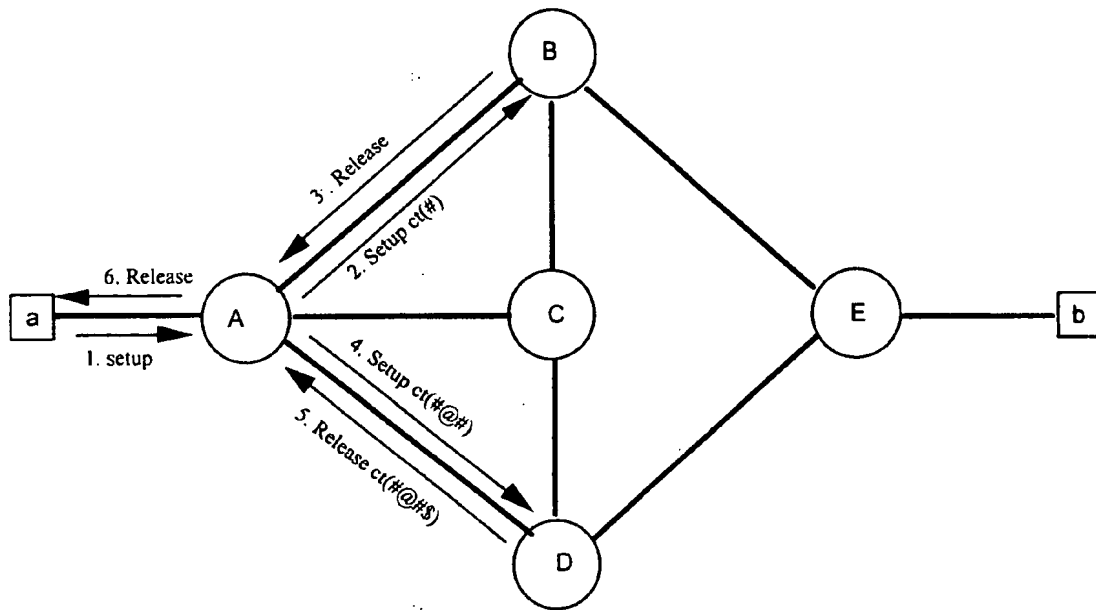


Figure 5

Markus & Olsch